

Política de Segurança da Informação

Versão: 09

Código: P-24

Elaborado por: TI

Revisado por: João dos Anjos

Aprovado por: TI

Publicado: Mar/2026

Sumário

1. Disposições Gerais	3
2. Propósito	4
3. Papéis e Responsabilidades	5
3.1 Colaboradores	6
3.2 Diretoria	7
3.3 Segurança da Informação	8
3.4 Tecnologia da Informação	9
3.5 Compliance	10
3.6 Jurídico	11
3.7 RH	11
4. Diretrizes Gerais	12
5. Proteção da Informação	14
5.1 Sigilo das informações decorrente da prestação de serviços	17
5.2 Gravação das ligações telefônicas	18
5.3 Monitoramento de mensagens eletrônicas	18
5.4 Inventário de Ativos	19
5.5 Senhas	19
5.6 Acesso e Restrição de Acesso	20
5.7 Uso de e-mail e internet	21
5.8 Ferramentas de Segurança	22
5.9 Descarte de equipamentos e destruição de informações	23
5.10 Gestão de Riscos	23
5.11 Gestão de Continuidade	24
5.12 Treinamentos	24
6. Serviços em Nuvem (Cloud)	25
7. Penalidades e Sanções	27
8. Disposições Finais	27
9. Regulamentação e Legislações Aplicáveis	28
10. Controle da Política	28

1. Disposições Gerais

Esta Política atende integralmente à Resolução CVM nº 35/2021, bem como demais normas da CVM, Bacen, B3 e BSM.

Aplica-se a colaboradores, diretores, prestadores de serviços, terceiros críticos e parceiros comerciais, Assessores de Investimentos e tem como objetivo proteger a informação em seus atributos de Confidencialidade, Integridade, Autenticidade, Disponibilidade e Registro de Incidentes

Informação é o conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenômeno ou evento e é ela que nos permite resolver problemas e tomar decisões, tendo em conta que o seu uso racional, é a base do conhecimento.

A informação é um dos principais ativos de nossa “Era” e necessita ser convenientemente protegida. A segurança de determinadas informações pode ser afetada por diversos fatores, tais como: comportamento dos usuários, ambiente/infraestrutura, sistemas de informação, ou ainda pessoas com objetivo de roubar, destruir ou modificar essas informações.

E apesar de cada dia mais as informações serem digitais, a Segurança da Informação não se resume apenas a proteção de sistemas computacionais, também se aplica a vários outros aspectos e formas de proteger, monitorar e cuidar de dados recebidos por meio de ligações telefônicas, documentos impressos, mensagens eletrônicas, entre outros.

Porém, nem toda informação é igual e precisa receber a mesma atenção. Por isso, as classificamos em diferentes níveis:

- **Confidencial** – informações que, em razão de lei, interesse público ou para a preservação de direitos individuais (privados), devam ser de conhecimento reservado e, portanto, precisam de medidas especiais de segurança e salvaguarda Ex.: qualquer informação de clientes;
- **Restrita** – informações que, por sua natureza, só podem ser divulgadas a um grupo restrito de pessoas. Ex.: informações sobre projetos específicos;
- **Uso Interno** – Informações que, por sua natureza, só podem ser divulgadas para uso interno da empresa. Ex.: documentos internos, políticas, procedimentos, manuais;

- **Pública** – Informações que podem ser divulgadas publicamente por não representar risco à empresa ou ser de interesse geral. Ex.: informações divulgadas ao público em geral.

Considerando a importância da informação para a continuidade do negócio, o conglomerado da Terra Investimentos adotou uma Política de Segurança da Informação que cumpre os requisitos legais rigorosos e fornece a garantia necessária de que os dados mantidos e processados pela organização são tratados com os padrões mais adequados para mantê-la segura.

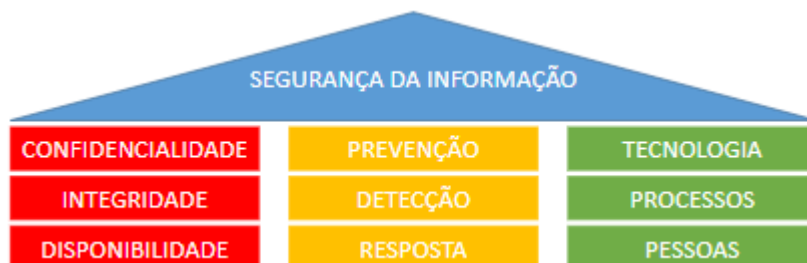
2. Propósito

Estabelecer controles de prevenção, detecção, resposta e recuperação de incidentes relevantes.

Aderência normativa: RCVN nº 35/2021 (arts. 5º, 33, 38, 41, 42 e 45), RCVN nº 50/2021 e Resolução Conjunta nº 13/2024 Bacen/CVM/Susep/Previc.

A Política de Segurança da Informação fornece orientação para a conduta considerada adequada ao negócio e ao objetivo, visão e valores do conglomerado da Terra Investimentos protegendo as informações contra destruição, modificação, divulgação e utilização indevida, quer sejam acidentais ou intencionais. Além disso, este documento fornece orientação para a correta guarda e armazenamento para consultas.

Esta Política garante que todos os sistemas informatizados e meios convencionais de processamento, comunicação e armazenamento de informações do conglomerado da Terra Investimentos, estejam devidamente assegurados de modo, a preservar sua Confidencialidade, Disponibilidade, Integridade da Informação, tendo em vista, à Prevenção, Detecção e Resposta à Incidentes. Para tanto, O Conglomerado Terra Investimentos, disponibiliza a Tecnologia necessária, define previamente os Processos, além de capacitar e treinar os colaboradores e/ou parceiros constantemente. Seguindo os pilares da Segurança da Informação:



- **Confidencialidade** - A Informação disponível somente às pessoas previamente autorizadas;
- **Integridade** - A informação de forma precisa, confiável, preservada, consistente e confiável;
- **Disponibilidade** - A informação disponível em tempo integral e estável;
- **Prevenção** - A proteção da Informação, com mecanismos de bloqueio e atualizações constantes;
- **Deteção** - O monitoramento constante da Informação, de modo a detectar eventuais ataques e/ou similares;
- **Resposta** - Atuações eminentes de resposta e/ou mitigação de eventuais ocorrências, que ofereçam riscos ao Ambiente de Tecnologia;
- **Tecnologia** - Todas as Ferramentas (Hardware e Software) que compõem o Ambiente de Tecnologia;
- **Processos** - Processos definidos, para a Segurança da Informação fluir de forma contínua;
- **Pessoas** - O principal pilar, com a capacitação e treinamento de pessoas.

Além disso, a adoção de uma política aumenta a conscientização dos colaboradores para evitar que eles possam inadvertidamente causar inconvenientes por meio da divulgação de dados, violação de leis ou ainda, evitar prejuízos financeiros e de reputação para a instituição.

3. Papéis e Responsabilidades

Todo colaborador é responsável pelo cumprimento das diretrizes da Política de Segurança da Informação do conglomerado da Terra Investimentos, sua ciência é documentada com a assinatura do Termo de Responsabilidade Ciência e Adesão à Documentação, que é assinado no ato da contratação. Por meio da

assinatura deste termo os colaboradores declaram a ciência e compromisso de seguir as regras de uso dos bens de informação a eles disponibilizados.

Além do comprometimento de todos os colaboradores do conglomerado da Terra Investimentos com a Segurança da Informação, algumas áreas são responsáveis por atividades específicas:

3.1 Colaboradores

- Cumprir integralmente esta Política, demais normas internas e legislações aplicáveis.
- Participar obrigatoriamente dos treinamentos anuais de Segurança da Informação, bem como reciclagens
- Assumir uma postura proativa no que diz respeito à proteção das informações do conglomerado da Terra Investimentos e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido aos sistemas de informação sob responsabilidade;
- Zelar continuamente pela proteção das informações do conglomerado da Terra Investimentos e de seus clientes, especialmente confidencial, contra acesso, modificação, destruição ou divulgação não autorizada;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados primariamente para fins profissionais do conglomerado da Terra Investimentos;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Atender às leis que regulamentam as atividades da empresa e seu mercado de atuação;
- Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento da Política de Segurança da Informação, e/ou das normas relacionadas;
- Comunicar imediatamente à área de Segurança da Informação quanto a eventos que envolvam segurança a informação como: E-mails suspeitos, sites suspeitos, arquivos suspeitos, perda de dados, divulgação de informação sensível na Internet, indisponibilidades, comportamento digital suspeito.

- Utilizar exclusivamente os recursos tecnológicos disponibilizados pela instituição, vedado o uso para fins pessoais, ilícitos ou incompatíveis com os objetivos do conglomerado
- Zelar pela guarda de senhas pessoais e intransferíveis, não sendo permitido o compartilhamento em nenhuma hipótese.
- Assinar o Termo de Confidencialidade e Responsabilidade no início da contratação.

3.2 Diretoria

A Diretoria é responsável pela governança e supervisão da Política, devendo:

- Nomear formalmente os Diretores Responsáveis por Segurança da Informação e por Continuidade de Negócios, declarando ausência de conflito de interesse, conforme art. 5º, §4º, I e II da RCVM 35/21;
- Os Diretores nomeados devem zelar pela efetividade da Política, supervisionar os testes de estresse e continuidade, e garantir que os incidentes relevantes sejam reportados tempestivamente aos órgãos reguladores e de administração
- Apoiar as políticas, as diretrizes e as normas de segurança da informação e continuidade de negócio
- Aprovar esta Política, suas revisões e adendos
- Prover os recursos necessários para garantir a eficácia das políticas;
- Assessorar o comitê quanto a qualquer decisão relacionada ao sistema de gestão segurança da informação e continuidade de negócio;
- Receber e deliberar sobre os relatórios:
 - Testes de estresse e de continuidade
 - Registros de incidentes relevantes, reportados imediatamente pela área técnica.
 - Receber relatórios de violações da política, diretrizes e das normas de segurança da informação, quando aplicável;
 - Receber relatórios de não conformidades;

- Tomar decisões referentes aos casos de descumprimento da política, diretrizes e das normas de segurança da informação, mediante a apresentação de melhorias contínuas.

3.3 Segurança da Informação

Responsável pela gestão técnica e operacional da Segurança da Informação, devendo:

- Elaborar, manter e atualizar o Programa de Segurança Cibernética, atendendo ao art. 45 da RCV 35/21.
- Conduzir testes de estresse anuais em sistemas críticos, documentando resultados e planos de ação (art. 33, §3º, II).
- Manter registro detalhado de incidentes, com logs sobre causa raiz, impacto, tempo de detecção, tempo de resposta e medidas de recuperação.
- Avaliar e classificar incidentes segundo critérios normativos: baixa, média, alta ou relevante (art. 41, III).
- Definir critérios técnicos de criptografia, backup, segregação de ambientes e trilhas de auditoria.
- Consolidar, manter e coordenar a elaboração e evolução, acompanhamento e avaliação do Comitê de Segurança da Informação e Continuidade de Negócio
- Convocar, coordenar e prover apoio às reuniões de comitê;
- Prover as informações de gestão de segurança da informação e continuidade de negócio;
- Executar projetos e iniciativas visando otimizar a segurança da informação e continuidade de negócio;
- Conduzir a Gestão, avaliação e tratamento de Risco ligados a segurança da informação e continuidade de negócio;
- Avaliar requisitos técnicos de segurança da informação e continuidade de negócio para implementação de novos controles e requisitos dentro do escopo de segurança da informação e continuidade de negócios;

- Criar e revisar os procedimentos de Segurança da Informação dentro do escopo do comitê de Segurança da Informação e Continuidade de Negócio;
- Atuar como ponto de orientação para outras equipes e gerências em assuntos relacionados à Segurança da Informação e Continuidade de Negócio;

3.4 Tecnologia da Informação

A área de TI deve fornecer infraestrutura segura e resiliente, incluindo:

- Executar patch management periódico e realizar varreduras de vulnerabilidades trimestrais.
- Garantir backup diário de sistemas críticos, com retenção mínima de 5 anos.
- Manter monitoramento contínuo de acessos, tráfego de rede e logs de sistemas.
- Implementar segregação de ambientes (produção, homologação, testes), conforme exigência do Manual de Acesso da B3 e item 136 do Roteiro PQO-BSM.
- Avaliar fornecedores de software e serviços de nuvem, assegurando cláusulas contratuais que prevejam notificação de incidentes em até 24 horas (art. 41, IV).
- Garantir que prestadores de serviços também assinem termos de confidencialidade antes de iniciarem atividades.
- Administrar acessos com base na Matriz de Segregação de Funções, garantindo o princípio do menor privilégio.
- Fornecer o suporte tecnológico necessário a todas as unidades do conglomerado da Terra Investimentos;
- Testar e ou promover testes exclusivos de novas versões de software e equipamentos para assegurar que elas tenham o menor risco e evitar possível falhas de segurança e ou funcionamento;
- Manter em seu quadro técnicos habilitados, treinados, conhecedores dos processos de negócios internos e capazes de identificar necessidades relacionadas a tecnologia ou riscos de segurança;

- Prospectar, avaliar e implantar softwares adquiridos de terceiros, bem como orientar os usuários na utilização dos sistemas utilizados pelo conglomerado da Terra Investimentos;
- Atender as novas necessidades de desenvolvimento de sistemas e a contratação de serviços de empresas especializadas devidamente habilitadas;
- Definir e manter políticas, normas e procedimentos referentes ao uso de recursos de informática, telefonia, mensageria e demais sistemas de negociação utilizados no conglomerado da Terra Investimentos;
- Definir controles específicos voltados para acesso, guarda e rastreabilidade física e digital de informações confidenciais, reservadas ou privilegiadas, observada a segregação por função e cargo de acordo com a necessidade das atividades de sócios, diretores, colaboradores e prestadores de serviços;
- Liberar ou não os acessos físicos e digitais aos colaboradores do conglomerado da Terra Investimentos de acordo com a Matriz de Segregação de Função e aprovação de custos se aplicável.

Nota: Gestor da Informação é o agente da instituição que possui conhecimento sobre processo e estrutura de determinado negócio e pode em conjunto com o Compliance e Segurança da Informação avaliar a elegibilidade dos acessos solicitados.

3.5 Compliance

A área de Compliance assegura a aderência regulatória e o monitoramento preventivo, cabendo-lhe:

- Monitorar comunicações corporativas (e-mails, gravações de voz, chats) em conformidade com a RCVM nº 50/2021, garantindo retenção mínima de 5 anos.
- Aprovar acessos excepcionais e acompanhar riscos de conflito de interesse.
- Validar que a PSI esteja alinhada às exigências de CVM, BSM e ANBIMA, emitindo parecer de conformidade.
- Acompanhar e auditar, em conjunto com Segurança da Informação, os testes de continuidade e estresse, registrando os resultados no Relatório de Controles Internos (RCI). Determinar a legitimidade (Não presente da

Matriz de Segregação de Função) e ou necessidade de todo acesso físico e digital, analisando antes de sua liberação ao usuário.

- Monitorar toda comunicação transmitida ou recebida por meio do ambiente tecnológico, informatizado, sistemas telefônicos, mensageria, comprovação de operações, evidências de processos, entre outras necessidades, principalmente, para fins de auditoria, ações judiciais e atividades investigativas, comprobatórias de registro entre outras.

3.6 Jurídico

O Jurídico deve apoiar a mitigação de riscos legais relacionados à SI:

- Assegurar que todos os contratos com terceiros críticos contenham cláusulas de proteção de dados, confidencialidade e notificação de incidentes em até 24h.
- Apoiar a área de Compliance na elaboração de comunicados obrigatórios a clientes e reguladores em caso de incidentes relevantes (art. 41, III da RCVM 35/21).
- Garantir que prestadores de serviços também assinem termos de confidencialidade antes de iniciarem atividades.
- Monitorar alterações legislativas e regulatórias em matéria de proteção de dados e cibersegurança, propondo adequações à PSI. Em conjunto com o Compliance, monitorar toda comunicação transmitida ou recebida por meio do ambiente tecnológico, informatizado, sistemas telefônicos, mensageria, comprovação de operações, evidências de processos, entre outras necessidades.

3.7 RH

O RH é responsável por assegurar a integração e desligamento seguro de colaboradores, incluindo:

- Obter assinatura do Termo de Confidencialidade até o 1º dia útil do colaborador.
 - Comunicar desligamentos imediatamente, para que a TI bloqueie acessos após a formalização.
-

- Incluir treinamentos de SI no processo de integração de novos colaboradores.
- Criar mecanismos para informar, antecipadamente aos fatos, ao canal de atendimento técnico mais adequado, alterações no quadro funcional do conglomerado da Terra Investimentos;
- Obter a assinatura do Termo de Responsabilidade ou Confidencialidade dos colaboradores, arquivando-o nos respectivos prontuários.

4. Diretrizes Gerais

A Terra Investimentos adota diretrizes estruturais de Segurança da Informação que asseguram a aderência à Resolução CVM nº 35/2021 e demais normas aplicáveis, estabelecendo padrões de governança, prevenção, detecção e resposta.

4.1 Estratégias de Segurança Preventiva

- Devem ser realizados testes de estresse anuais nos sistemas críticos da instituição, abrangendo, no mínimo, os sistemas de Cadastro de Clientes e Suitability, Registro e Roteamento de Ordens, Controle de Limites de Risco, Liquidação de Operações, Custódia de Ativos, Conciliação Posicional, Plataformas de Negociação Eletrônica e Gateways de Comunicação com a B3/BSM, conforme definido pelo Roteiro PQO da BSM.
 - Os testes devem simular cenários de indisponibilidade, falhas operacionais, ataques cibernéticos e sobrecarga transacional, com elaboração de relatório técnico contendo resultados, falhas identificadas e plano de ação.
 - Os resultados devem ser formalmente reportados à Diretoria em até 30 dias após a execução, em conformidade com o art. 33, §3º, II da Resolução CVM nº 35/2021. A elaboração, treinamento e divulgação das estratégias de segurança devem ser realizadas de forma contínua, com revisão anual.

- A estratégia deve contemplar riscos físicos, lógicos e cibernéticos, incluindo cenários de ataques terroristas e ciberterroristas, alinhados ao Plano de Continuidade de Negócios.
- Todos os colaboradores devem ser comunicados das alterações de forma tempestiva, com comprovação de ciência

4.2 Procedimentos e Ferramentas de Proteção Ativa

- Devem ser utilizados controles de proteção ativa contra fraudes, vazamentos de dados, ataques cibernéticos, phishing, ransomware e ataques de negação de serviço (DDoS).
- O conglomerado deve implementar ferramentas de antivírus, firewall de última geração, SIEM, DLP, criptografia e autenticação multifator, garantindo monitoramento 24x7.
- A integridade da marca e a reputação institucional devem ser protegidas por controles de monitoramento de mídias sociais e canais públicos, com respostas a incidentes reputacionais em até 24h após detecção.

4.3 Controles de Segurança sobre Ativos e Instâncias

- Todos os ativos físicos, digitais e lógicos da Terra Investimentos (informações internas e de clientes, sistemas de negociação, telefonia, mensageria, sistemas de custódia e liquidação) devem possuir controles de segurança formalmente documentados.
- Deve ser mantido inventário trimestral de ativos de informação, atualizado e auditável.
- O acesso a sistemas críticos deve observar o princípio do menor privilégio e estar sujeito a revisão anual obrigatória.

4.4 Uso Exclusivo dos Ativos Corporativos

- Os ativos, sistemas e informações do conglomerado só podem ser utilizados em benefício da instituição e de seus clientes.
-

- É vedada a utilização de recursos de TI, telefonia ou mensageria para fins particulares, atividades ilícitas ou incompatíveis com o objeto social da instituição.
- O descumprimento será tratado como infração grave, sujeito a medidas disciplinares e comunicação à Diretoria, podendo configurar incidente de segurança relevante.

4.5 Dever de Zelo dos Colaboradores

- Todos os colaboradores têm responsabilidade solidária de zelar pelos recursos sob sua custódia.
- Cada colaborador deve:
 - Bloquear o computador ao se ausentar de sua estação de trabalho.
 - Proteger dispositivos móveis corporativos com senha e criptografia.
 - Notificar imediatamente a área de Segurança da Informação sobre qualquer violação, perda ou suspeita de comprometimento.
- O não cumprimento ensejará medidas administrativas e, em caso de dolo ou negligência grave, aplicação das penalidades previstas na legislação (inclusive CLT, art. 482).

5. Proteção da Informação

O conglomerado da Terra Investimentos adota uma série de medidas para assegurar que a Política de Segurança da Informação esteja em conformidade com as melhores práticas de mercado e com as normas da Resolução CVM nº 35/2021, da Resolução Conjunta nº 13/2024 Bacen/CVM/Susep/Previc e dos roteiros da BSM Supervisão de Mercados, sendo estabelecido que:

- Os usuários são responsáveis pelas informações armazenadas nos equipamentos que utilizam, devendo priorizar o armazenamento seguro em pastas de rede corporativa, sujeitas a backup automatizado, trilha de auditoria e segregação de acessos, sendo vedado o uso de dispositivos pessoais ou não monitorados.
- A Terra Investimentos compromete-se a adotar critérios técnicos para preservar a integridade, confidencialidade e disponibilidade das informações, incluindo:

- execução de backups diários com retenção mínima de cinco anos;
 - uso obrigatório de criptografia em repouso e em trânsito para dados sensíveis;
 - aplicação de autenticação multifator em sistemas críticos;
 - monitoramento contínuo 24x7 de acessos, tráfego e registros de logs;
 - realização de auditorias periódicas dos controles de segurança, com reporte anual à Diretoria
- Toda aquisição ou locação de recursos de informática (equipamentos, softwares, sistemas, nuvens de serviços) é previamente consentida pela área de Tecnologia da Informação, mediante aprovação prévia da Diretoria.
 - Todo recurso de informática é inventariado e qualquer alteração em sua configuração original só pode ser realizada pela área da Tecnologia da Informação.
 - Todos os programas de computador desenvolvidos para o conglomerado da Terra Investimentos são de propriedade da mesma e obedecem aos critérios legais e melhores práticas com modelos de desenvolvimento seguro.
 - É responsabilidade do usuário não instalar programas em condição ilegal de uso ou não autorizados pela área de Tecnologia da Informação.
 - A área de Tecnologia da Informação realiza o monitoramento da instalação de programas ilegais ou não autorizados.
 - A aquisição, homologação e instalação de licenças de programas segue normas e procedimentos definidos pela área de Tecnologia da Informação do conglomerado da Terra Investimentos.
 - As licenças de programas de computador usados por terceiros são de inteira responsabilidade deles, mas devem obedecer a critérios mínimos de Segurança da Informação.
 - Os usuários são responsáveis pelas informações armazenadas nos equipamentos que utilizam, bem como a manutenção dos arquivos armazenados em pastas. O modo mais seguro de armazenar documentos e informações é utilizando pastas e diretórios disponíveis em rede.

O conglomerado da Terra Investimentos compromete-se a manter a integridade das informações, para isso adota uma série de critérios, utiliza-se de ferramentas que tem por objetivo garantir a segurança das informações em posse da instituição.

5.1 Comunicação de Incidentes

- Registro obrigatório.
 - Todo incidente de segurança da informação deve ser imediatamente registrado em sistema de gestão de incidentes (logging) pela área de Segurança da Informação, contendo: data/hora, causa raiz (quando identificada), impacto, sistemas/processos afetados, tempo de detecção, tempo de resposta, medidas de contenção/recuperação e status do plano de ação.
- Critérios de relevância. Para fins desta Política, são incidentes relevantes aqueles que:
 - causem indisponibilidade superior a 2 horas em sistemas críticos (Cadastro de Clientes e Suitability, Registro e Roteamento de Ordens, Controle de Limites de Risco, Liquidação de Operações, Custódia de Ativos, Conciliação Posicional, Plataformas Eletrônicas de Negociação e gateways de comunicação com B3/BSM);
 - resultem em vazamento de dados pessoais ou sensíveis de clientes;
 - comprometam a integridade de registros de operações ou posições de custódia;
 - representem risco à continuidade de negócios ou à reputação institucional.
- Classificação.
 - A classificação em baixo, médio, alto ou relevante seguirá os critérios do art. 41, III e IV, da Resolução CVM nº 35/2021 e normas internas correlatas.
 - Prazo de comunicação à CVM. Incidentes relevantes devem ser comunicados à CVM em até 24 (vinte e quatro) horas a contar da identificação, nos termos do art. 41, §4º, da RCVM nº 35/2021.

- Demais comunicações. Quando aplicável, incidentes relevantes também devem ser comunicados à BSM, ANBIMA, Bacen e outros reguladores competentes, bem como aos clientes afetados (se houver impacto direto), de forma clara, objetiva e tempestiva.
- Conteúdo mínimo da comunicação. A comunicação regulatória deve conter, no mínimo: descrição do evento, data/hora, escopo e sistemas afetados, impacto estimado (inclusive em clientes), medidas de contenção adotadas, plano de recuperação e ações de prevenção/mitigação futuras; atualizações devem ser encaminhadas sempre que surgirem informações relevantes adicionais.
- Responsabilidades.
 - A Segurança da Informação lidera a resposta e o registro; a TI executa contenção e recuperação técnica; Compliance/Jurídico revisam as comunicações regulatórias e coordenam eventual comunicação a clientes; áreas de Relacionamento/Atendimento apoiam o contato com partes afetadas.
- Terceiros críticos.
 - Contratos com terceiros relevantes devem conter cláusula de notificação à Terra em caso da detecção de incidente, disponibilizando evidências técnicas necessárias para investigação e comunicação regulatória.
- Evidências e guarda.
 - Todos os registros, logs e evidências (tickets, relatórios forenses, prints, artefatos) devem ser preservados por mínimo de 5 (cinco) anos, assegurando a rastreabilidade.
- Testes e exercícios.
 - A instituição realizará exercícios periódicos (ao menos anuais) de simulação de incidentes cibernéticos e de continuidade para validar tempos de resposta e fluxos de comunicação; os resultados serão reportados à Diretoria.

5.2 Sigilo das informações decorrente da prestação de serviços

No mercado no qual o conglomerado da Terra Investimentos está inserido, o sigilo proteção das informações é imprescindível. Por isso, todas as informações classificadas nas disposições gerais deste documento recebem atenção em relação ao seu uso e divulgação.

Além disso, no conglomerado da Terra Investimentos são tratadas também como informações confidenciais e restritas as seguintes, sem prejuízo de outras em ocorrências de novos negócios:

- Registros de ocorrências.
- Estudos internos usados para tomadas de decisão.
- Acordos financeiros em geral.
- Documentos de terceiros e clientes.
- Workflows internos.
- Dados estatísticos gerenciais diversos.
- Toda informação cadastral de clientes.
- Base de cadastro, financeira, controladoria e contábil.
- Inteligência de Negócio
- Contas a pagar e folha de pagamento, serão divulgadas apenas com partes autorizadas. Dados de operações de clientes e posições de custódia.

5.3 Gravação das ligações telefônicas

- O conglomerado da Terra Investimentos mantém sistema de gravação dos ramais que são objetos de monitoramento por amostragem, coordenados pela área de Compliance, que podem ser disponibilizadas entre um dia e uma semana, em caso de necessidade de restauração de Backup.
- As gravações são armazenadas durante 5 anos.

5.4 Monitoramento de mensagens eletrônicas

- Os sistemas de mensageria e outros são gravados e disponibilizados sempre que solicitado.
 - As mensagens são mantidas armazenadas durante 5 anos.
-

5.5 Inventário de Ativos

O conglomerado da Terra Investimentos mantém inventário atualizado dos ativos de informação contendo recursos de hardware, software, aplicações de negócio, equipamentos de rede, recursos humanos, instâncias virtuais em nuvem, instalações físicas e itens de configuração relevantes para a empresa como terceiros e fornecedores.

5.6 Senhas

- As senhas são pessoais e intransferível, é expressamente proibido o compartilhamento de senha pessoal. Todos os colaboradores que têm acesso a contas de sistemas deverão ser claramente identificados;
- Todas as senhas em nível de usuário, por exemplo, senha de rede deve ser alteradas, no máximo, a cada noventa dias, exceto nos casos de senhas para plataformas eletrônicas;
- As senhas não devem ser anotadas ou inseridas em mensagens de e-mail ou outras formas de comunicação eletrônica;
- As senhas devem possuir no mínimo seis caracteres contendo letras maiúsculas, números e caracteres especiais;
- As senhas devem possuir histórico mínimo de seis senhas utilizadas, exceto nos casos de senhas para plataformas eletrônicas;
- As senhas nunca devem ser escritas ou armazenadas em sistemas sem criptografia;
- As senhas serão bloqueadas após cinco tentativas incorretas;
- O desbloqueio do usuário será efetuado pelo administrador da rede. Em plataformas eletrônicas o desbloqueio deverá ser mediante a confirmação de dados do usuário, tais como, dados pessoais e cadastrais;
- Constitui obrigação exclusiva do usuário, zelar pela guarda e conservação de sua senha, cabendo ao usuário informar ao departamento de Tecnologia sobre suspeitas e uso, ou efetivo ou indevido. O uso indevido da senha ou credencial de acesso por terceiros não exime a responsabilidade do usuário;

- Todas as senhas devem ser tratadas como informações confidenciais do conglomerado da Terra Investimentos;
- Exceções a esta norma podem ser concedidas de acordo com cada cenário, havendo a necessidade de tratamento registrado de exceções.

5.7 Acesso e Restrição de Acesso

O conglomerado da Terra Investimentos restringe o acesso as informações e áreas físicas e eletrônicas apenas para colaboradores autorizados, fazendo o uso do princípio do menor privilégio. Por isso:

- Os crachás são pessoais e intransferíveis, sendo vedado o empréstimo.
- Os acessos as áreas são previamente autorizadas pelo Compliance e liberado pela área de Tecnologia da Informação (Suporte), que mantém os controles monitorados em sistema.
- Não é permitido dar carona ou a entrada de pessoas não autorizadas nos ambientes controlados por dispositivos de controle de acesso (salvo exceções autorizadas quanto a visitas de fornecedores e clientes).
- Não é permitida a violação dos dispositivos de controle de acesso por qualquer motivo, exceto por manutenção.
- A concessão de acesso à rede, programas, cadastros sistemas são feitas por meio de análise da Matriz de Segregação de Função de modo a identificar a legitimidade do acesso em questão.
- Todo acesso a informações do conglomerado da Terra Investimentos, feitos fora da matriz, devem ser autorizados pelo Compliance e Gestor da Informação.
- Todos os acessos são passíveis de auditoria seja navegação, acesso físico e acesso lógico.
- Não é permitida a utilização de aparelho celular, *tablets*, *smartwatches* de propriedade particular nos ambientes destinados à realização das operações de mercado.
- Não é permitido a utilização de dispositivos não monitorados (gravados) na realização de operações de mercado.

- Todos os acessos a sistemas estão sujeitos à revisão minimamente anual para verificação do perfil do usuário que devem ser validadas pelos respectivos gestores.
- Todos os casos de desligamentos e/ou transferência de colaboradores devem ser imediatamente comunicados por Recursos Humanos para que seus acessos sejam bloqueados e/ou reformulados.
- Não é permitido o desbloqueio de portas (salvo exceção quando acompanhado por responsável por motivos previamente avisados como manutenções).
- Não é permitida a permanência de portas abertas nos ambientes operacionais, administração de fundos e ambiente computacional do conglomerado da Terra.

Todos os acessos físicos e lógicos devem ser solicitados para a área de Suporte. Para conceder o acesso, a área de Suporte verifica as permissões constantes na Matriz de Segregação de Funções e Acessos. Caso a solicitação não esteja prevista na Matriz, a área de Suporte solicita autorização para a área de Compliance.

A área de Compliance analisará caso a caso em conjunto com o gestor do solicitante. Caso a solicitação seja para acesso a informações confidenciais, reservadas ou privilegiadas que sejam essenciais para o desempenho das atividades, o usuário deverá assinar novo termo de confidencialidade sobre as informações a que terá acesso. Caso seja para uso temporário, os acessos devem ser retirados assim que as atividades tenham sido encerradas.

5.8 Uso de e-mail e internet

A comunicação indevida por e-mail, sistema de mensagens ou acesso a sites não autorizados pode comprometer a Segurança da Informação do conglomerado da Terra Investimentos, sendo assim são adotadas algumas premissas como:

- O acesso à internet dentro das dependências do conglomerado da Terra Investimentos é classificado e bloqueado/permitido com base em
-

categorias de Website com bloqueios em especial a (chats, redes sociais de entretenimento, webmails etc.)

- Apenas o e-mail corporativo pode ser utilizado para troca de mensagens referentes a assuntos do conglomerado da Terra investimentos.
- Todos os colaboradores devem utilizar o e-mail disponibilizado pelo conglomerado da Terra Investimentos para fins profissionais, sendo proibido o uso para fins particulares.
- O acesso a sites disponíveis na rede mundial de computadores é restrito visando a vulnerabilidade de alguns sites como rede sociais, sites de compra, entre outros.
- O conglomerado da Terra Investimentos reserva-se o direito de monitorar o acesso à Internet e envio de mensagens eletrônicas, com o objetivo de proteger os dados da instituição.
- As caixas de e-mail utilizadas para recebimento e transmissão de ordens, instruções e confirmações são armazenadas pelo período de 5 anos.

5.9 Ferramentas de Segurança

A fim de evitar o vazamento de informações, fuga de dados, a integridade e guardas destas, é essencial a utilização de ferramentas tecnológicas destinadas a proteção dos sistemas informatizados, do conglomerado da Terra Investimentos:

- Backups regulares.
- Segurança de antivírus.
- Gerenciamento de Patch – proteção contra ameaças.
- Gestão de vulnerabilidade varredura do ambiente.
- Monitoramento comportamento suspeito (Internet, E-mail, Mensagens, Redes Sociais etc.).
- Criptografia.
- Bloqueio de gravações (saídas USB, pen drives, HD etc.).

O tráfego de dados, preservação de documentos e rastreabilidade das informações são garantidas com a utilização do Sistema especializado que:

- Rastreia o ciclo de vida de um documento (qualquer alteração realizada por funcionários e clientes pode ser verificada).
- Rastreio de envio do documento para e-mails particulares, túneis etc.
- Mantém arquivos, documentos e dados armazenados criptografados.

5.10 Descarte de equipamentos e destruição de informações

Toda mídia e papel deverá ser descartada quando se tornar desnecessária. A mídia não deverá ser reutilizada, doada para caridade ou descartada sem a devida autorização da área Tecnologia da Informação. Para minimizar o risco de divulgação acidental de informação sigilosa, a área Tecnologia da Informação deverá garantir a execução de uma forma segura de descarte (ou seja, incineração, fragmentação ou limpeza completa), destruindo completamente e de maneira irreversível toda e qualquer informação do conglomerado da Terra Investimentos. O descarte de papel deverá ser feito após a trituração de seus conteúdos de modo que se tornar ilegível e/ou irrecuperável.

A reutilização, venda ou doação assistencial de computador fora de uso, poderá ocorrer, se não houver qualquer risco de exposição de dados sigilosos, ou danos organizacionais potenciais à informação previamente abrigada nesses sistemas.

5.11 Gestão de Riscos

As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação do conglomerado da Terra Investimentos deverão considerar, prioritariamente, os objetivos estratégicos, os processos críticos, os requisitos legais e a estrutura da empresa, além de estarem alinhadas a esta Política de Segurança da Informação. Esse processo deverá ser contínuo e aplicado na implementação, operação, manutenção, controle e melhoria contínua do Sistema de Gestão de Segurança da Informação e do Sistema de Gestão de Continuidade de Negócio.

5.12 Gestão de Continuidade

O conglomerado da Terra Investimentos deverá elaborar, implementar, operar, manter, controlar e melhorar continuamente a Gestão de Continuidade de Negócio, que deverá ser composto, no mínimo, pelos planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos processos críticos de informação e a recuperação das atividades essenciais:

- Os planos de continuidade de negócios (PCN) devem ser testados ao menos uma vez ao ano, abrangendo cenários de indisponibilidade de sistemas, ataques cibernéticos, falhas físicas e desastres.
- Os resultados dos testes devem ser documentados em relatório formal e reportados à Diretoria e ao Conselho de Administração em até 30 dias após sua execução, em conformidade com o art. 38, §3º da Resolução CVM nº 35/2021.
- Documentação dos procedimentos e informações necessárias para que o conglomerado da Terra Investimentos mantenha seus processos de informação críticos e a continuidade de suas atividades vitais, num nível previamente definido, em casos de crises, desastres ou catástrofes.
- Documentação dos procedimentos e informações necessárias para que o conglomerado da Terra Investimentos operacionalize o retorno das atividades críticas à normalidade.
- Os planos definidos deverão ser testados e revisados periodicamente, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos processos críticos de informação.

5.13 Treinamentos

O conglomerado da Terra Investimentos adota as melhores práticas de mercado, por isso promove a divulgação interna de sua Política de Segurança da Informação e oferece treinamento sobre o tema para todos os colaboradores e para garantir o sigilo das informações os colaboradores são orientados a:

- Todos os colaboradores, diretores, terceiros críticos e prestadores de serviços devem realizar treinamento anual obrigatório em Segurança da Informação.
- Em caso de incidente relevante, deve ser promovida reciclagem obrigatória em até 30 dias após a ocorrência, com foco nas falhas identificadas.
- O conteúdo mínimo deve abranger: classificação da informação, boas práticas de senhas, uso de e-mail e internet, prevenção de phishing, LGPD, resposta a incidentes, continuidade de negócios e cultura de cibersegurança.
- A participação deve ser registrada eletronicamente e os comprovantes de conclusão guardados por 5 anos como evidência para fins regulatórios

6. Serviços em Nuvem (Cloud)

A Terra Investimentos cumpre todas as regulamentações vigentes, para contratação de serviços de processamento e armazenamento de dados de computação em nuvem.

No cumprimento das obrigações na contratação e manutenção dos serviços em Cloud. A área de TI Infraestrutura deve seguir os procedimentos e manuais abaixo, listados:

- Práticas de Governança:
 - Política de Segurança Cibernética;
 - Política de Backup;
 - Política de Continuidade de Negócio;
 - Política de Gerenciamento de Mudança;
 - Política de Privacidade;
 - Plano de Respostas à incidentes.
 - Capacitação de colaboradores
 - SOD

7. Programa de Segurança Cibernética

O conglomerado da Terra Investimentos mantém um Programa de Segurança Cibernética, em conformidade com o art. 45 da Resolução CVM nº 35/2021, com o objetivo de assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações e dos sistemas críticos da instituição. O Programa contempla, no mínimo, as seguintes diretrizes:

- Identificação e avaliação de riscos: a instituição realiza avaliação periódica de riscos cibernéticos, utilizando metodologias com foco nos sistemas críticos de cadastro, ordens, liquidação, custódia e conciliação. Os resultados são documentados e apresentados à Diretoria.
- Medidas de mitigação: são implementados controles técnicos e administrativos para reduzir a probabilidade e o impacto de ataques cibernéticos, incluindo firewall de última geração, SIEM, DLP, antivírus corporativo, criptografia, autenticação multifator e gestão de vulnerabilidades, com revisões trimestrais.
- Verificação da eficácia: a efetividade dos controles é avaliada por meio de testes de penetração periódicos, auditorias internas e externas, e análises de logs de segurança, com evidências mantidas por mínimo de 5 anos.
- Monitoramento contínuo: responsável por monitorar eventos de segurança, detectar comportamentos suspeitos e acionar respostas imediatas a incidentes.
- Tratamento e recuperação de incidentes: são mantidos planos formais de resposta a incidentes, atualizados e testados regularmente, assegurando que falhas sejam contidas, investigadas e reportadas à Diretoria e aos órgãos reguladores, quando aplicável.
- Treinamento e conscientização: todos os colaboradores, diretores, terceiros críticos e prestadores de serviços participam de programa anual de capacitação obrigatória.

9. Penalidades e Sanções

São consideradas violações à política, às diretrizes, às normas ou aos procedimentos de segurança da informação ou continuidade de negócio as seguintes situações, não se limitando às mesmas:

- Quaisquer ações ou situações que possam expor o conglomerado da Terra Investimentos à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos críticos de informação;
- Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais, informações de clientes ou outras informações confidenciais sem a permissão expressa do Proprietário da Informação;
- Uso de dados, imagens, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos, como o Código de Ética, e externos, ou de exigências de organismos reguladores da área de atuação do conglomerado da Terra Investimentos;
- A não comunicação imediata às áreas de Segurança da Informação de quaisquer descumprimentos da política, dos critérios, de normas ou de procedimentos de Segurança da Informação, que porventura um colaborador venha a tomar conhecimento ou chegue a presenciar.

O não cumprimento dos itens descritos acima, ainda que por mero desconhecimento, sujeitará o infrator a sanções administrativas, incluindo, a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

10. Disposições Finais

Esta Política de Segurança da Informação deverá ser comunicada a todos os colaboradores do conglomerado da Terra Investimentos a fim de que seja atendida dentro da organização. O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação ou Continuidade de Negócio, acarretará violação às regras internas da empresa e sujeitará o colaborador às medidas administrativas e

legais cabíveis, podendo envolver advertência, suspensão, rescisão contratual ou outras medidas cabíveis conforme legislação vigente, além de aplicação das punições previstas no artigo 482 da CLT.

11. Regulamentação e Legislações Aplicáveis

A Terra Investimentos cumpre todas as regulamentações vigentes.

12. Controle da Política

Esta Política está aprovado pela Diretoria, encontra-se disponível e foi comunicado as pessoas vinculadas relevantes para o necessário cumprimento.

Será revisada periodicamente ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
